

### IN THE CLAIMS:

Claims 1-6, 9-15, 18-23, and 26-33 are amended. No claims are cancelled or added.

All pending claims and their present status are produced below.

- 1 1. (Currently amended) A method for providing ~~[[a]]~~ unique ~~identification~~  
2 identifications of monitored network data instances flowing across various  
3 connections between networked devices, the unique ~~identification~~ identifications  
4 being derived from information contained entirely within each instance of ~~the~~  
5 network data, the method comprising:  
6 using ~~at least one~~ a monitoring device to monitor a network data instance flowing  
7 across ~~at least one~~ a data connection;  
8 deriving from the data instance certain information which collectively provides a  
9 unique identification of the network data instance;  
10 assembling the derived information into an input string for a hash function; and  
11 using ~~the~~ an output string of the hash function as a signature which represents a  
12 unique identifier of the network data instance.
- 1 2. (Currently amended) The method according to Claim 1, wherein the deriving step  
2 includes:  
3 deriving from the data instance a source and destination address for the data instance;  
4 deriving from the data instance a source and destination port associated with the  
5 networked devices; and  
6 deriving from the data instance ~~at least one~~ a sequence number associated with data  
7 instance.

- 1 3. (Currently amended) The method according to Claim 1, which further includes:  
2 attaching the signature to ~~at least one~~ a data report associated with the network data  
3 instance; and  
4 transmitting the data ~~reports~~ report and ~~the signatures~~ signature from each ~~the~~  
5 monitoring device to a central collecting device.
- 1 4. (Currently amended) The method according to Claim 3, wherein a timestamp is  
2 further associated with each ~~the~~ the data report before it is transmitted to the central  
3 ~~collector~~ collecting device.
- 1 5. (Currently amended) The method according to Claim 3, wherein the central  
2 collecting device uses the ~~signatures~~ signature to eliminate duplicate data reports that  
3 might come in from different monitoring devices positioned at different locations on  
4 ~~the a~~ a network.
- 1 6. (Currently amended) The method according to Claim ~~[[1]]~~ 2, wherein ~~the~~ the network  
2 data instances ~~are~~ include data packets as part of a TCP/IP (Transmission Control  
3 Protocol/Internet Protocol) client-server network.
- 1 7. (Original) The method according to Claim 6, wherein the source and destination  
2 addresses include a client IP address and a server IP address.
- 1 8. (Original) The method according to Claim 7, wherein the source and destination port  
2 include a client port number and a server port number.
- 1 9. (Currently amended) The method according to Claim 2, wherein the ~~at least one~~  
2 sequence number includes a client sequence number or a server sequence number.

- 1 10. (Currently amended) The method according to Claim 9, wherein the ~~at least one~~  
2 sequence number includes both a client sequence number and a server sequence  
3 number.
- 1 11. (Currently amended) The method according to Claim ~~[[2]]~~ 1, wherein the input string  
2 ~~information~~ does not include a sequence ~~numbers~~ number.
- 1 12. (Currently amended) The method according to Claim ~~[[11]]~~ 1, wherein the network  
2 data instances ~~are~~ include datagrams as part of a UDP/IP (User Datagram  
3 Protocol/Internet Protocol) network.
- 1 13. (Currently amended) The method according to Claim 1, which further includes ~~[[:]]~~  
2 truncating the signature to include fewer bits than the hash function output string.
- 1 14. (Currently amended) The method according to Claim 1, which further includes ~~[[:]]~~  
2 adding flag bits to the signature which indicate ~~the~~ a type of application associated  
3 with the network data instance.
- 1 15. (Currently amended) The method according to Claim 3, wherein the ~~monitor~~  
2 monitoring device serves as a data reduction device for data report and signature  
3 information being sent to the central ~~data collector~~ collecting device.
- 1 16. (Original) The method according to Claim 1, wherein the monitoring device operates  
2 to directly monitor the network data.
- 1 17. (Original) The method according to Claim 1, wherein the monitoring device operates  
2 to indirectly monitor the network data.
- 1 18. (Currently amended) An apparatus for providing ~~[[a]]~~ unique ~~identification~~  
2 identifications of monitored network data instances flowing across various  
3 connections between networked devices, the unique ~~identification~~ identifications

4 being derived from information contained entirely within each instance of the  
5 network data, the apparatus comprising:  
6 ~~at least one~~ a monitoring device positioned to monitor a network data instance  
7 flowing across ~~at least one~~ a data connection;  
8 a hash function device having an input string and an output string, the input string  
9 assembled from certain information derived from the network data instance,  
10 the information collectively providing a unique identification of the network  
11 data instance;  
12 wherein the output string is used as a signature which represents a unique identifier of  
13 the network data instance.

1 19. (Currently amended) The apparatus according to Claim 18, wherein the information  
2 derived from the network data instance includes at least:  
3 a source and destination address derived from the network data instance;  
4 a source and destination port associated with the networked devices; and  
5 ~~at least one~~ a sequence number associated with network data instance.

1 20. (Currently amended) The apparatus according to Claim 18, which further includes:  
2 ~~at least one~~ a data report associated with the network data instance, the signature  
3 being attached to the data report; and  
4 a central collection device that receives ~~transmitted~~ the data reports report and  
5 ~~signatures~~ the signature from each the monitoring device.

1 21. (Currently amended) The apparatus according to Claim 20, wherein a timestamp is  
2 further associated with each the data report before it is transmitted to the central  
3 ~~collector~~ collection device.

- 1 22. (Currently amended) The apparatus according to Claim 20, wherein the central  
2 ~~collecting~~ collection device uses the ~~signatures~~ signature to eliminate duplicate data  
3 reports that might come in from different monitoring devices positioned at different  
4 locations on ~~the~~ a network.
- 1 23. (Currently amended) The apparatus according to Claim 19, wherein the network data  
2 instances ~~are~~ include data packets as part of a TCP/IP (Transmission Control  
3 Protocol/Internet Protocol) client-server network.
- 1 24. (Original) The apparatus according to Claim 23, wherein the source and destination  
2 addresses include a client IP address and a server IP address.
- 1 25. (Original) The apparatus according to Claim 24, wherein the source and destination  
2 port include a client port number and a server port number.
- 1 26. (Currently amended) The apparatus according to Claim 25, wherein the ~~at least one~~  
2 sequence number includes a client sequence number or a server sequence number.
- 1 27. (Currently amended) The apparatus according to Claim 26, wherein the ~~at least one~~  
2 sequence number also includes both a client sequence number and a server sequence  
3 number.
- 1 28. (Currently amended) The apparatus according to Claim ~~[[19]]~~ 18, wherein the input  
2 string ~~information~~ does not include a sequence ~~numbers~~ number.
- 1 29. (Currently amended) The apparatus according to Claim 28, wherein the network data  
2 instances ~~are~~ include datagrams as part of a UDP/IP (User Datagram Protocol/Internet  
3 Protocol) network.
- 1 30. (Currently amended) The ~~method~~ apparatus according to Claim 18, wherein the  
2 signature is truncated to include fewer bits than the hash function output string.

1 31. (Currently amended) The ~~method~~ apparatus according to Claim 18, wherein flag bits  
2 are added to the signature which indicate ~~the~~ a type of application associated with the  
3 network data instance.

1 32. (Currently amended) The ~~method~~ apparatus according to Claim 20, wherein the  
2 ~~monitor~~ monitoring device serves as a data reduction device for the data report and  
3 the signature ~~information~~ being sent to the central ~~data-collector~~ collection device.

1 33. (Currently amended) A method for providing ~~[[a]]~~ unique ~~signature~~ signatures of  
2 monitored network data packets flowing across various connections between  
3 networked devices, the unique ~~signature~~ signatures being derived from information  
4 contained entirely within each instance of the network data ~~packet~~ packets, the  
5 method comprising:  
6 using ~~at least one~~ a monitoring device to monitor a network data packet flowing  
7 across ~~at least one~~ a data connection;  
8 deriving from the data packet a source and destination address for the data packet;  
9 deriving from the data packet a source and destination port associated with the  
10 networked devices;  
11 deriving from the data packet ~~at least one~~ a sequence number associated with the data  
12 ~~instance~~ packet;  
13 assembling the derived addresses, ports, and ~~at least one~~ the sequence number  
14 ~~information~~ into an input string for a hash function;  
15 using ~~the~~ an output string of the hash function as ~~the~~ a signature which represents a  
16 unique identifier of the network data packet;

17 attaching the signature to ~~at least one~~ a data report associated with the network data  
18 packet; and  
19 transmitting the data ~~reports~~ report and ~~signatures~~ signature from ~~each~~ the monitoring  
20 device to a central collecting device for analysis.